PRIVACY LAW: RIGHT TO BE FORGOTTEN IN INDIA

*Prashant Mali**

I. INTRODUCTION

The "right to forget" refers to the already intensively reflected situation that a historical event should no longer be revitalized due to the length of time elapsed since its occurrence; the "right to be forgotten" reflects the claim of an individual to have certain data deleted so that third persons can no longer trace them. Therefore, the right to be forgotten is based on the autonomy of an individual becoming a right holder in respect of personal information on a time scale; the longer the origin of the information goes back, the more likely personal interests prevail over public interests.

The right to be forgotten was recognized for the first time in India through the judgment delivered by Karnataka High Court in the matter of *Sri Vasunathan vs The Registrar-General* in 2017. A decade ago, however, a similar term, namely the "right to forget," was already a topic of debate. But viewed precisely, the active and the passive side of the "forget" medal are not identical, and the right to be forgotten should not be confused with the right to forget as happens frequently in blog discussions.

Basically, "Right to be forgotten" or "Right to be Erased" provides a right to individual to request for removal of his/her personal data floating around through Internet. The simple rule behind data erasure is that whoever is using the data has volunteer consent from the data owner. So, when the consent is withdrawn, the owner has a right to

have his data erased.[1] Also when the data controller has no legal right to process the data, the data should be erased.[2] In case of data erasure, whoever has the data access or whoever is processing the data has to erase it and have to remove any links, copies or replication of data. The origin of this right is traced from French jurisprudence on the "right to oblivion"; which was to make social integration easy for offenders who had served their sentence on basis of the publication of information of their crime.[3] Based on French jurisprudence, European Union Data Protection Directive, 1995 acknowledged the right to be forgotten, by introducing Article 12, which specifies that the member state should provide people to control, ratify, erase or block data related to them.

The significant technical challenge for implementation of "Right to be forgotten" is defining "personal data". According to Article 17 of European Union (EU) Directives, the term "personal data" means *any information relating to the individual*. Such a definition raises ambiguities on issues like collective information - information which may not identify any person individually but pointed towards the family. The identification of personal data becomes more complicated when it comes to erasure of derived data about individuals used in statistics or in another form of aggregated information. Once, there are reasonable grounds for data erasure, it is not clear practically how this erasure will be enforceable. According to EU, every individual has a right to control his or her private data, especially if they are not public figures.[4]

*Prashant Mali is the president and founder of Cyber Law Consulting (Advocates & Attorneys), Mumbai. The author may be reached at cyberlawconsulting@gmail.com.

[1]General Data Protection Regulation (EU) No. 2016/679 of 27 April 2016, Right to erasure, art. 17, 19, (hereinafter "GDPR").

[2]*Id*. art. 18, 19.

[3]Loc.gov. *Online Privacy Law: France, Law* Library of Congress (2018). https://www.loc.gov/law/help/online-privacy-law/france.php.

[4]*Supra* note 1, art. 18,19.

II. RIGHT TO BE FORGOTTEN UNDER EU DIRECTIVES

To make "*right to be forgotten*" enforceable EU introduced (Directive 95/46/EC) in 1995. In the EU in particular, this "*right to be forgotten*," was gaining increasing traction as a potential foundation of privacy regulation (Bennett, 2012). According to Vice President of the European Commission, Vivean Reding, the EU data protection reform, which was well overdue, should include provision for removal of online personal information.[5] In 2014, the Court of Justice of the European Union (CJEU) established the 'Right to be Forgotten' and accordingly, "*Every individual has the right – under certain conditions – to ask search engines to remove links with personal information about them.*"[6] As of March 2017, Europeans had submitted over 715,000 requests to deactivate two million URLs. Google has deleted over forty-three percent of those, approximately 732,000 links.[7] In fact, according to EU regulations, social media networks also need to erase personal data of individuals when asking under laws allowing people the "*Right to be Forgotten*".[8] At the same time, the Court's decision has stirred debates focused on the tension the decision raised between a person's right to privacy and freedom of

[5]Viviane Reding, Vice President, (EU), *The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age*, 5 (Jan. 22, 2012), http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/26&format=PDF.

[6]HUFFPOST, *Do we Have a Right to be Forgotten?* https://www.huffingtonpost.com/lindsay-hoffman/do-we-have-a-right-to-be_b_7812564.html [last visited Feb. 26, 2018].

[7]Weaver, M., *Google 'learning as we go' in row over right to be forgotten*. THE GUARDIAN. https://www.theguardian.com/technology/2014/jul/04/google-learning-right-to-be-forgotten [last visited 26 Feb. 2018].

[8]Catherin Stupp, *Germany set to fine social media platforms millions over hate speech*, EURACTIV, https://www.euractiv.com/section/digital/news/germany-plans-to-fine-social-media-platforms-millions-over-hate-speech/.

expression. The CJEU offered little guidance in determining when personal information is subject to mandatory erasure due to irrelevance or inadequacy. The opinion on "right to be forgotten" differs immensely between America and EU countries. According to America, transparency, the right to freedom of speech and expression is a priority. The publication of truthful information about individual or corporation is favoured by America. But, the European court of justice legally freezes the "*Right to be Forgotten*" as a human right in the *Costeja* case[9] against Google.

In the year of 2010, Mr. Costeja file a complaint against Google and Spanish Newspaper at National Data Protection Authority of Spain. In his complain, he mentioned that when he searches his name on Google, the search results show a link of newspaper article about a property sale made by him to replay his personal debts.

The authority dismissed the complaint against newspaper as they had the legal obligation to publish the property sale information. But authority allowed the complaint against Google.

In this matter, Google argued that as no physical server in Spain held the data and data are processed outside the European Union, it does not come under European Data Protection Directives. As a matter of practice, when Google receives a takedown notice for linking to infringing content, it removes those links from all of its sites across the world, so could the same not be done for private information?[10]

[9]Google Spain SL &Anr. V. Agencia Española de Protección de Datos&Anr, ECLI:EU:C:2014:317**,** Grand Chamber, (May 13, 2014), http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&docid=152065.

[10]Manjoo, F., *Right to Be Forgotten' Online Could Spread*, NYTIMES. https://www.nytimes.com/2015/08/06/technology/personaltech/right-to-be-forgotten-online-is-poised-to-spread.html [last visited Feb. 24, 2018].

The Court of Justice of EU finally stated that: The search engine companies are controllers of their services[11] and whoever promote and market their services within EU, the Data Protection Directives ("DPD") applies to them and consumer have the right to request such search engine companies to remove links or information associated with him/her. After this again the matter comes back to The Court of Justice of EU for removing the links from global domains rather than geo-limiting delinking.[12] After this decision, other search engine companies like Bing have already begun implementing the decision in Europe.[13]

There is one more case of Europe against Facebook, which does not talk about "*right to be forgotten*" but it gives an approach for erasing data.[14] This case basically explains erasing data by not displaying it to anybody. In this case was filed by Max Schrems, who asked Facebook to provide him all his personal information had on him. Initially, he received PDF file more than 1000 pages. This file also includes information, which he thought was deleted. Therefore, he decided to file a complaint against Facebook Ireland in front of the Irish Data Protection Commissioner.

Initially, he had filed 22 complaints against Facebook, which includes subjects such as shadow profiling, excess personal data, not removing data, face recognition. Addition complaints were filed in the year of

[11]Supra Note 1, ⁋⁋ 32, 33, 34.

[12]*CNIL, Right to delisting: Google informal appeal rejected,* https://www.cnil.fr/en/right-delisting-google-informal-appeal-rejected-0 [last visited Feb. 27, 2018].

[13]*See*, for example, Luciano Floridi, *Right to be forgotten poses more questions than answers*, THE GUARDIAN, https://www.theguardian.com/technology/2014/nov/11/right-to-be-forgotten-more-questions-than-answers-google.

[14]The Data Protection Commissioner v. Facebook Ireland Limited &Anr., High Court Ireland, Oct. 3, 2017, http://www.europe-v-facebook.org/sh2/HCJ.pdf.

2011, which contains subjects such as: tracking user's location via like button, picture link deletion, frequently changing policies.

The main issue, in this case, was that the data i.e. posts, pock, chat messages, friends, were not deleted by Facebook even though he had clicked on the delete button. Instead of removing data from a server, Facebook had made data in "invisible" mode. Even images were not deleted, only links of the images were removed.

After a long legal battle, the procedure ended in 2014 with the decision by Max Schrems, to withdraw the 22 complaints made initially.

Following the withdrawal of the complaint, an Austrian style class action lawsuit was started against Facebook in August 2014 with the aim "to make Facebook finally operate lawfully in the area of data protection".[15] This complaint has mainly focus on following points:

1. The Data use policy of Facebook, which is not legally valid under EU law.
2. There is no effective consent to many types of data use.
3. Support of the NSA's 'PRISM' surveillance programme.[16]
4. Tracking Internet user's actions on external websites.
5. Monitoring and analyzing users through "Big data techniques".
6. Unlawful introduction of 'Graph Search'
7. Unauthorized transfer of user data to external applications.

[15]EUROPE-V-FACEBOOK, http://europe-v-facebook.org/EN/Complaints/Class_Action/class_action.html [last visited Feb. 23, 2018].

[16]Top secret program allowing the NSA access to data from Google, Facebook, Apple and other major IT-companies.

On 1st of July 2015, The Court of Vienna rejected the case on procedural grounds, because Max Schrems used Facebook account for commercial promotions of his publications. The case transfers the case to a higher tribunal, and Max Schrems said he wants to appeal the decision. This suit is still under procedure at Austrian Supreme Court, so the clear conclusion is yet to be declared.

Analysis: In Facebook case, the interesting part is, Facebook has shown two different approaches to erase data from public domain: 1) Making Data invisible, 2) deleting only links to a file. Facebook just remove the links or make data invisible to user who wants to delete it. The same logic applies to everyone who was accessing or had permission to access such data. For example, if the user's profile is a public profile then people from public domain has access to profile or if the profile is private then his friends can access such profile. Once the user erases the data, Facebook still has the access to the data, as the data is not originally deleted from the Facebook database. Thus, if think from the perspective of the users who had access to the data before deletion, the data is deleted. But, the data is only removed from access domain.

Thus, removing links to the files or making data status invisible can deny the access to data. This approach is similar to the Google Case. But in case of Facebook no one can access erased data by using different permutations. Google actually removed the data access from the specific environment rather than deleting it from the public domain. Making data invisible works for the environment, which has control over access to data. In case of Google, it does not have any control over who has access to the data. Whereas, Facebook has a specific environment, which has control over who has access to data.

III. RIGHT TO BE FORGOTTEN WITH RESPECT TO DATA RETENTION & GDPR

As pointed out by Korenhof et al. (2014) the timing of data retention plays a part in this debate as longer periods of data retention make it difficult for digitally recorded actions to be forgotten. Privacy laws encompass any policy or legislation that governs the use and storage of personal information about individuals whether by the government, public, or private entities. As Hetcher (2001) points out, the Internet can often lead to a "threat to personal privacy" due to the "ever-expanding flow of personal data online." This notion of privacy and security of personal data has become one of the more significant public policy concerns generated by the Internet, leading to "legal and regulatory challenges" (Salbu, 1998).

To unify data protection for all within the European Union, GDPR was introduced on 27th April 2016. The GDPR will be applicable in European Countries form 25th May 2018. The aim of introducing GDPR is to give control of personal data to the citizens and to simplify data erasure process and regulatory environment for international business. According to Article 17 of GDPR, *the right to be forgotten* means:

- Data Subjects have the right to obtain erasure from the data controller, **without undue delay**, if one of the following applies:

    1. The controller doesn't need the data anymore

    2. The subject withdraws consent for the processing with which they previously agreed to (and the controller doesn't need to legally keep it [N.B. Many will, e.g. banks, for 7 years.])

    3. The subject uses their right to object (Article 21) to the data processing

4. The controller and/or its processor is processing the data unlawfully

5. There is a legal requirement for the data to be erased

6. The data subject was a child at the time of collection (See Article 8 for more details on a child's ability to consent)

- If a controller makes the data public, then they are obligated to take reasonable steps to get other processors to erase the data, e.g. A website publishes an untrue story on an individual, and later is required to erase it, and also must request other websites erase their copy of the story.

Exceptions to above provision:

The Data might not be erased if any of the following applies:

- For exercising the right of freedom of expression and information;
- For compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- For reasons of public interest in the area of public health
- For archiving purposes in the public interest, scientific or historical research purposes or statistical purposes
- For the establishment, exercise or defence of legal claims.

More generally, the length of data retention has become an issue in this debate over privacy. The question is whether the benefits of privacy (less data retention) for consumers outweigh any potential costs to consumers (lower quality search results). The right to erasure does not provide absolute "*right to be forgotten*". Every individual has a right to erase personal data and prevent processing of data save for but in certain circumstances.[17] European filtering of Internet content worldwide through the right to be forgotten effectuates international censorship in the guise of privacy. As per Article 17, GDPR has a data retention provision when it requires. For example, GDPR has provision for employee data retentions. GDPR contains provisions for in what circumstances, which personal data should be retained and for what time period.

Before GDPR, UK already has their data protection regulations. Similar to UK regulations GDPR has introduce some regulation in terms of employee data retentions which are as below[18]:

- The right to be informed: "The employer obelized to inform employee about how personal data will be used"
- The right to ratification: inaccurate or incomplete data needs to be rectified.
- The right to be forgotten: No longer required data needs to be deleted from employer's database.
- The right to block or suppress from processing: The employee should have right to block or suppress from processing his/her personal data.
- The right to data portability: Employee should have right to reuse his/her personal data for personal purpose during certain circumstances.

[17]According to Dr. Guy Bunker, SVP Products at Clearswift (Data Security Company)

[18]As defined in article by Ronan Daly Jermyn, A leading law firm in Chambers of Europe.

To implement right to erasure properly, every organization needs to implement an accurate mechanism to erase data absolutely from their system on demand by their customers or clients meaning that the data should not exist in backups as well. [19] According to GDPR, if you are using a third-party service for data storage then also, the organization needs to be aware of what is the mechanism third party is using at the time of data erasure. If the third party does any mistake in data erasure then also the organization will also be jointly liable for such mistake. The GDPR will not only apply to employers processing the personal data of their employees, but also to HR service providers that process such data on behalf of the employer ("data processors"). [20]

Articles 17 (2) and 18 (1a) mandate that data processing after retention period is also not permissible, meaning that once the data has to be deleted then data controller cannot use such data for other purposes.

One challenge faced by the Indian legal system is that currently, most privacy laws at the federal level predate the technologies, such as the Internet, that raise privacy issues. In recent years, innovations such as behavioral advertising, location-based services, social media, mobile apps, and mobile payments lead to heated debates over an individual's privacy and security. Given that most innovations and regulations occur in the EU, we study here the effects of changes in those policies abroad and their implications for the India Internet.

[19]D. Froud, *GDPR: Does the Right to Erasure Include Backups? - Froud on Fraud*, FROUD ON FRAUD. http://www.davidfroud.com/does-right-to-erasure-include-backups/.

[20]AMCHAM.BE, *The new EU data protection regime from an HR perspective*. http://www.amcham.be/publications/amcham-connect/2016/march/fieldfisher-gdpr-data-protection-human-resources-hr-perspective.

IV. EFFECT OF RIGHT TO BE FORGOTTEN ON MACHINE LEARNING

In machine learning regarding the deletion of privacy data, the right to be forgotten is the right to support one's informational autonomy by giving the decisive power to data providers. The management of private data and handling of deletion requests of such data are the challenges facing machine learning. Now, removing personal information from prominent search engines like Google challenges fundamental aspects of machine learning. One major question is what will be the effect of data removal on knowledge base machine learning algorithm. As per the previous approach continuously increasing the amount of information will enhance the performance of the result.[21] So, deletion of information from existence will reduce the quality of results even more. So, to avoid this drawback machine learning algorithm should be made more powerful which can make information more generalized in analytical results. To implement this idea, organizations need to use the approach of encoding sensitive data with some privacy protection means and then analysed by machine learning algorithm and then only the information should available for inspection.[22]

Now, one interesting fact about the Mr. Costeja's case is that the original information about Mr. Costeja is never removed from the database. At present, one can still find an online version of the newspaper. So, what machine learning does is once the app done with the data object and memory is freed or erased, the data does not disappear immediately. The chunk of memory is put into a linked list and then it will be processed and then make a software memory part

[21]B. Malle, P. Kieseberg, E. Weippl, A. Holzinger: *The Right to Be Forgotten: Towards Machine Learning on Perturbed Knowledge Bases*, Workshop on Privacy Aware Machine Learning (PAML), August 2016.

[22]Green, A. and Green, A., *The Right to Be Forgotten and AI*. VARONIS BLOG. https://blog.varonis.com/right-forgotten-ai/ [last visited Feb 23, 2018].

available for re-use. So, at a certain point of time data does not dispose of instantly. Now machine learning works with a large number of data, due to which the software continuously allocating and deleting data, sometimes data might be present in disposal queue.

As per GDPR, if it is necessary to remove personal information on request, one cannot defend on technical complexity. So, there needs to be some technical solution to make data completely invisible. So the now machine learning algorithm should be based on any anonymity technique or pseudonymization to avoid storing identifiable data, to implement right to be forgotten.[23] According to the technology experts, to make data unavailable form the public domain, there are four factors, which need to be taken into consideration: 1) Time[24] 2) Meaning of Information 3) Regularity 4) Space. To identify or to make a decision which data needs to be deleted when *right to be forgotten*' accessed by any person the above four factors needs to be analysed for data erase.

V. RIGHT TO BE FORGOTTEN IN INDIA

However, In India there are no specific data protection laws, so ad-hoc judicial attention of the court is sought. In the writ petition *Sri Vasunathan v The Registrar-General*[25] before the Karnataka High Court, the Court observed that "*This would be in line with the trend in western countries of the 'right to be forgotten' in sensitive cases*

[23]Malle, B, Kieseberg, P, Weippl, E & Holzinger, A 2016, *The right to be forgotten: Towards Machine Learning on perturbed knowledge bases*, 251-266, Springer Lecture Notes in Computer Science LNCS 9817. Springer International, Privacy Aware Machine Learning (PAML) for health data science, Salzburg, Austria.

[24]*See* Sartor, G. *Timing the Right to Be Forgotten: A Study into "Time" as a Factor in Deciding About Retention or Erasure of Data* (2018).

[25]Sri Vasunathan v. The Registrar General & Ors., http://www.iltb.net/2017/02/karnataka-hc-on-the-right-to-be-forgotten/

involving women in general and highly sensitive cases involving rape or affecting the modesty and reputation of the person concerned." Hence, the Court directed its registry that petitioner's daughter's name should not reflect in the case-title of the order or in the body or the order in the criminal petition. The woman's father had approached the high court for seeking the directions to remove woman's name from the earlier order passed by the high court. The petitioner had stated that his daughter's relationship with her husband and her reputation in society will get affected if her name remains associated with her earlier case.

Similarly, Once Justice Sanjay Kishan Kaul delivered his opinion on right to forgotten and he stated, "The right of an individual to exercise control over his personal data and to be able to control his/her own life would also encompass his right to control his existence on the Internet" [26]

In contrast with above-mentioned opinion, Gujarat High Court *Dharamraj Dave v. State of Gujarat*[27]) pointed out that there is no attracted law to remove judgment from Google search or Indian Kanoon and petitioner does not have sufficient arguments to prove "uploading judgment on the Internet is a violation of Article 21 of the Constitution." These cases demonstrate the lack of legal framework and the inability of the judiciary in interpreting the right to be forgotten. So, India requires specific Data protection Laws to protect right to be forgotten.

In 2017, in Justice K S Puttaswamy's case, the "*right to be forgotten*" defined by The European Union Regulations, 2016, has been recognized. The following are the considerations made by the Supreme Court:

[26]Justice K. S. Puttaswamy & Ors. v. Union of India, (2017) 10 SCC 1.
[27]Dharmraj Bhanushankar Dave v. State of Gujarat, 2015 SCC OnLine Guj 2019.

1. Children around the world have access to the digital media. They are constantly making their footprints on social media networking. They are passing the data with chat, Bluetooth, web downloading, Emails, Facebook, Google, Hotmail, and Instagram. They should not be affected by their childish mistake or naivety, their entire life. So, the parents of such children or the person can request for remove data or personal information regarding their childhood or their children.[28].

2. People change and every individual should be able to move forward in life and should not be stuck by the mistake done in past. Every individual should have the capacity to change his/her beliefs and improve as a person. The individual should not live in the fear that the view expressed by them will stay forever with them.

3. Whereas this right to control the dissemination of personal information does not amount to total erasure history, as this right is a part of right to privacy and should be balanced against other fundamental rights like right to freedom of expression, or freedom of media.

4. Thus, Right to be forgotten means, when the data of any person is no longer required or who expects that his/her personal data will be no longer stored or processed then he/she should be able to remove it from the system where the information is no longer necessary, relevant or is incorrect or is illegitimate. But, Right to be forgotten does not mean to remove data or personal information, which is necessary for exercising right of freedom of expression and information,

[28]Michael L. Rustad, SannaKulevska, *Reconceptualizing the right to be forgotten to enable transatlantic data flow*, 28 HARV. J.L. & TECH. 349.

> for the performance of the task carried out in public interest, in public interest in the area of public health, scientific or historical research purpose, exercise or defense for legal claim.[29]

As a part of privacy, every individual should be able to control his/her personal data and to be able to control his/her life encompasses his right to control his/her existence on the Internet. But this does not mean that a criminal can obliterate his past, but there are various degrees of mistake, small or big, it cannot be said that a person should be profiled to the extent many times more than his mistake.

After the *Justice K.S Puttaswamy* judgment, Government of India decided to constitute a committee of Experts to regime Data Protection Laws in India. So, under the chairmanship of former Supreme Court Justice Shri B N Srikrishna a committee has released a white paper on Data Protection Framework for India on November 27, 2017.[30]

According to the white paper, the consent should be one of the grounds for data processing. But, here the consent should be valid. As the committee noticed that one of the three Internet users across the world is the child under the age of 18. So, a data protection law must be efficient to protect their interests, while considering their vulnerability and exposure to risks online.

The committee has also commented on Purpose of Data Collection. According to White Paper, there should be some specific purpose for personal data collection. Also, the collected personal data should be erased once the purpose is fulfilled. The committee also mentioned in

[29]Justice K S Puttaswamy & Ors. v. Union of India, (2017) 10 SCC 1, ¶ 69.
[30]*White paper of the Committee of Experts on a Data Protection Framework for India*, Government of India, http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final _v2.1.pdf.

the report that, the person should have a right to confirm, access, and rectify his or her own data.

Also, the white paper talks about the issues with right to be forgotten provisions under data protection law. Accordingly the right to be forgotten should not conflict with freedom of speech and expression and while formulating a right to be forgotten, it is necessary to identify the third party can be held liable for failing to comply with erasure request or not.

VI. CONCLUSION

"Right to be forgotten" is becoming very important for the legal aspect as well as technical aspect. Due to technical complications, legal provisions for such right are also getting complexes. Now as "Right to be Forgotten" is increasingly being viewed as a part of the right to privacy. When we talk about "Right to be forgotten", the information will be considered true so the right to free expression and publication could not be overshadowed by "Right to be Forgotten".[31] In India, this debate is still continuing as India does not has any specific provision for providing such a "Right to be forgotten". India is still dependent on ad-hoc jurisprudence to access this right. As the Union Government of India is making laws for Data Protection and the Committee has recognized this right in Chapter 10 of White paper, it is expected that there will be provision for such a right in the upcoming law on data protection.

[31]Justice K. S. Puttaswamy & Ors. v. Union of India, (2017) 10 SCC 1, ¶ 68.